Robert C. Schubert (No. 62684)
Willem F. Jonckheer (No. 178748)
Noah M. Schubert (No. 278696)
Cassidy Kim (No. 315236)
Schubert Jonckheer & Kolbe LLP
Three Embarcadero Ctr Ste 1650
San Francisco, CA 94111-4018
Ph: 415-788-4220
Fx: 415-788-0161
rschubert@sjk.law
wjonckheer@sjk.law
nschubert@sjk.law
ckim@sjk.law

Attorneys for Plaintiff Asha Goldweber and the Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO / OAKLAND DIVISION

Asha Goldweber, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

Equifax, Inc.,

Defendant.

Case No.

Complaint for Violation of Cal. Civ. Code §§ 1798.80 *et seq.*, Violation of Cal. Bus. & Prof. Code §§ 17200 *et seq.*, Negligence, and Negligence *Per Se*

Class Action

Demand for Jury Trial

Table of Contents

Upon personal knowledge as to her own acts and status, and based upon her investigation, her counsel's investigation, and information and belief as to all other matters, plaintiff Asha Goldweber, on behalf of herself and all others similarly situated, alleges:

SUMMARY OF ACTION

1. This is a class action brought on behalf of California and other U.S. citizens who had their personally identifiable information ("PII") stolen by criminals as a direct result of Equifax's failure to adhere to reasonable, industry-standard security practices.

2. On September 7, 2017, Equifax announced that hackers had exploited a website application vulnerability ("the data breach") and obtained the PII of approximately 143 million Americans, including over 15 million Californians. As a result, the hackers obtained names, birthdays, social security numbers ("SSNs"), addresses, and in some cases, driver license numbers. Equifax also disclosed that the hackers accessed credit card numbers for approximately 209,000 U.S. consumers, in addition to certain dispute documents for approximately 182,000 U.S. consumers.

3. Equifax first discovered the intrusion on July 29, 2017. The company reported that the hackers took advantage of a known vulnerability in an open-source software package called Apache Struts (CVE-2017-5638). Apache had released software updates back on March 8, 2017 to address this vulnerability, but Equifax failed to implement the patch until more than four months later when it discovered the data breach. As a result, the hackers gained unauthorized access to Equifax's computer systems from May 13, 2017 through July 30, 2017.

4. In response, Equifax has not provided adequate measures for consumers to protect themselves from further harm. Equifax waited nearly six weeks after it discovered the data breach to publicly disclose the incident. During this time, millions of consumers remained unaware that their PII had been stolen and that it was vulnerable to misuse by bad actors. When it disclosed the data breach, Equifax set up a separate website at www.equifaxsecurity2017.com that consumers could utilize to identify whether they are victims of the data breach. The website requires

consumers to enter in their last name and the last six digits of their SSN. Due to the sensitive nature of the information requested, consumers have to trust they are giving their PII to the right party. However, Equifax breached that trust by inadvertently directing consumers to a phishing website instead.

5. Equifax had a statutory obligation to protect the PII of its consumers yet failed at every step to prevent, detect, or limit the scope of the data breach. Equifax was well aware of the growing threat of cyber attacks and was on full notice of its security vulnerabilities, having recently experienced a breach of its TALX division in March 2017. Nonetheless, Equifax, *inter alia*, (a) failed to implement software updates for known a security vulnerability, (b), failed to detect unauthorized intrusions into its computer systems, and (c) failed to timely notify consumers of the data breach and provide them with adequate protection measures.

6. Defendant concealed the weaknesses in its security systems, was negligent in safeguarding consumer data, and violated California statutes, including the California Data Breach Act, CAL. CIV. CODE §§ 1798.80 *et seq.*, and the California Unfair Competition Law ("UCL"), CAL. BUS. & PROF. CODE §§ 17200 *et seq.* As a direct result of the data breach, Plaintiff and the Class suffered damages, including (a) costs associated with the detection and prevention of identity theft and unauthorized use of their personal and financial information and (b) the imminent and impending costs from future fraud and identity theft.

PARTIES

7. Plaintiff Asha Goldweber ("Goldweber") is a citizen of California and a resident of Oakland, California. Upon information and belief, Ms. Goldweber's Social Security number and other PII were exposed by Equifax. Ms. Goldweber first learned of this breach from news reports. Concerned her information may have been comprised, Ms. Goldweber visited Equifax's website dedicated to providing information about the breach, trustedidpremier.com, to determine if her PII was compromised. The response from Equifax's website indicated that Ms. Goldweber's personal information was exposed as a result of Equifax's data breach.

8. Defendant Equifax, Inc. ("Equifax") is a Georgia corporation with its principal place of business in Atlanta, Georgia. Equifax maintains extensive contacts within the State of California. Equifax provides consumer reporting and monitoring services to California residents, maintains offices in California, employs workers in California, and advertises in California.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because (a) this is a class action in which the matter in controversy exceeds $5 million, exclusive of interests and costs; (b) there are more than one hundred class members; and (c) Plaintiff and the class are citizens of different states than at least one defendant, satisfying the minimal diversity requirement.

10. This Court has personal jurisdiction over Defendant because Defendant has sufficient minimum contacts with California and/or Defendant otherwise purposely avails itself of the markets in California by conducting consumer reporting and monitoring services in California, maintaining offices in California, employing workers in California, and advertising in California. Defendant's wholly-owned subsidiary, TrustedID, Inc., which Defendant directed consumers to for credit monitoring services post-breach, is headquartered in Palo Alto, California. Defendant's purposeful availment of the markets in California renders the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

11. Venue is proper under 28 U.S.C. § 1391 because (1) Defendant is subject to personal jurisdiction in the Northern District of California, and (2) a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District. Defendant provides credit reporting and monitoring services in this District, maintains offices in this District, employs workers in this District, and advertises in this District. Plaintiff is a resident of this District, and Plaintiff's PII was collected by Defendant in this District.

12. Intradistrict Assignment: Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Francisco and Oakland Division of the Northern District of California (the "Division") is

proper, because a substantial part of the events or omissions which give rise to the claims occurred in this Division. Defendant provides credit reporting and monitoring services in this Division, maintains offices in this Division, employs workers in this Division, and advertises in this Division. Plaintiff is a resident of this Division, and Plaintiff's PII was collected by Defendant in this Division.

FACTUAL ALLEGATIONS

Equifax Collects Personally Identifiable Information on Millions of Consumers

13. Equifax is one of three primary credit reporting agencies ("CRAs") in the United States and "organizes, assimilates and analyzes data on more than 820 million consumers" worldwide.[1] Together, with the other two major CRAs, Equifax has gathered credit histories and identifying information for nearly every adult in the United States.

14. As part of its credit reporting business, Equifax is given access to a wide range of personal information to make creditworthiness judgments on millions of consumers. These judgments directly affect decisions on employment, loans, and housing applications. In fact, Equifax touts itself as part of the "essential decision-making fabric" for "many of the world's leading businesses in the financial services, retail, auto, mortgage, communications/utilities and other sectors."[2]

15. Equifax offers credit monitoring and identity theft services for individual consumers as well. These personal solutions require the provision of PII, including names, addresses, birthdays, and SSNs, in addition to continued access to the consumers' financial activities as part of the monitoring services.

---

[1] *Company Profile*, EQUIFAX, http://www.equifax.com/about-equifax/company-profile (last visited Sep. 21, 2017).

[2] *Consumer Information Solutions*, EQUIFAX, http://m.equifax.com/consumer/en_us (last visited Sep. 21, 2017).

16. Equifax also solicits credit grantors and other businesses to furnish customer data on a regular basis. In doing so, Equifax seeks to maintain the integrity of its consumer files.[3] To the extent that Equifax's market value relies heavily on the quality of the consumer information it has amassed, Equifax has every economic incentive to maintain the most amount of information on the largest number of consumers.

17. By collecting and storing such extensive and detailed consumer data, Equifax obligates itself to use every reasonable means available to protect this data from falling into the hands of criminals. Equifax's failure to implement reasonable security measures led to the biggest cyber attack of 2017.

Equifax Is Put on Notice of the Threat of Sophisticated Cyber Attacks

18. Over recent years, companies in various industries have experienced data breaches of increasing magnitude, involving the theft of PII and other sensitive information that threaten the security and economic health of consumers. Businesses and regulators alike have noted that the data breaches are not limited to select industries, but instead, impact data stewards across all sectors, including healthcare providers, financial service companies, retail businesses, and government entities.

19. At the same time, there were important trends that should have placed Equifax on high alert. In California, for example, malware and hacking attacks posed the greatest threats, both in the number of breaches and the number of records breached.[4] Even more, SSNs were the data type most often breached.[5]

20. In response, regulators have called for the implementation of reasonable security measures across all industries. The Federal Trade Commission highlighted that security is not a

---

[3] *Guidebook for Prospective Data Furnishers*, EQUIFAX, http://www.equifax.com/assets/USCIS/data_furnisher_guidebook.pdf (last visited Sep. 21, 2017).

[4] *California Data Breach Report*, OFFICE OF THE ATTORNEY GENERAL, CALIFORNIA DEPARTMENT OF JUSTICE (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf ("CA Breach Report").

[5] *Id.*

one-and-done deal. Instead, reasonable security requires ongoing vigilance, including the need to update and patch third-party software.[6] Likewise, the California Attorney General's Office has noted the importance of continuously assessing vulnerabilities and patching holes.[7]

21. Equifax has also acknowledged security as a key tenet of its role as a trusted data steward, highlighting the need for "continued investments to address critical data security throughout the company."[8]

22. Despite its representations, Equifax itself has a history of failing to adequately protect consumer data. Prior to this data breach, it had been vulnerable to data breaches numerous times, including a recent hack in March 2017 that implicated W-2 tax records through Equifax's subsidiary TALX. In response to that incident, which resulted from hackers resetting employees' four-digit PIN numbers, security researchers condemned Equifax's failure to implement even the most basic security measures, such as two-factor authorization, to protect such sensitive information.

23. In light of growing industry-wide concern over cyber attacks, including numerous high profile incidents, the previous attacks against Equifax, and the warnings that regulators issued cautioning companies to take increased protections for SSNs, particularly against hacking attacks, Equifax *knew* or *should have known* that its security practices were completely inadequate to combat the threat.

Equifax's Inadequate Security Practices Resulted in One of the Largest Data Breaches in U.S. History

24. The Equifax data breach "represents one of the largest risks to personally sensitive information in recent years, and is the third major cybersecurity threat for the agency since

---

[6] *Start With Security*, FEDERAL TRADE COMMISSION, (Jun. 2014), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[7] CA Breach Report, *supra* note 4.

[8] Investor Relations Report, EQUIFAX (Jun. 2017), https://investor.equifax.com/~/media/Files/E/Equifax-IR/documents/presentation/investor-relations-presentation-june-2017.pdf.

2015."[9] The sheer scale of the data breach has security experts operating under the "assumption that everyone's Social Security number has been compromised and their identity data has been stolen."[10]

25. On September 7, 2017, Equifax first disclosed that its computer systems had been breached, nearly six weeks after the company discovered the intrusion in late July. Equifax disclosed that the breach occurred between May 13, 2017 and July 30, 2017, resulting in the PII theft of approximately 143 million Americans, including over 15 million Californians.[11] That amounts to approximately a two and a half month delay between when the data breach began and Equifax first detected it.

26. As a result of the data breach, the hackers obtained names, birthdays, SSNs, addresses, and in some cases, driver license numbers. The attackers also gained unauthorized access to credit card numbers for approximately 209,000 U.S. consumers, in addition to certain dispute documents containing PII for approximately 182,000 U.S. consumers.[12]

27. This massive data breach could have been entirely prevented, especially given the prior attacks Equifax faced and the extensive warnings provided by regulators and industry players. Yet Equifax did not take the necessary steps to protects its sensitive consumer data and computer systems from attack.

28. First, Equifax should have —but did not— implement a software patch for a known application vulnerability. Equifax initially reported that the hackers broke into the

---

[9] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, THE NEW YORK TIMES (Sep. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[10] Lily Hay Newman, *The Equifax Breach Exposes America's Identity Crisis*, WIRED (Sep. 8, 2017), https://www.wired.com/story/the-equifax-breach-exposes-americas-identity-crisis/.

[11] Press Release, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sep. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832 ("Equifax Press Release 2"); Press Release, Attorney General Becerra Issues Consumer Alert Following Equifax Data Breach, OFFICE OF THE ATTORNEY GENERAL, CALIFORNIA DEPARTMENT OF JUSTICE (Sep. 10, 2017), https://www.oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach.

[12] *Id.*

computer's systems by "exploit[ing] a U.S. website application vulnerability to gain access to certain files."[13] The company later explained that the vulnerability pertained to the Apache Struts web application framework.[14] This Apache vulnerability allows hackers to remotely access and execute commands on web servers.[15]

29. Importantly, this was a widely known vulnerability for which Apache promptly released software updates back on March 8, 2017.[16] However, security experts warned early on that there would be delays in patching, because the process was "labor intensive and difficult," requiring system managers to "download[] an updated version of Struts and then us[e] it to rebuild all apps that used older, buggy Struts versions."[17] Nevertheless, when Equifax discovered the data breach, it took its systems offline and was able to implement the patch within just a day before putting the systems back online.[18] Unfortunately, the patch came more than four months after the update was made available, and only after millions of Americans' PII were stolen.

30. Second, Equifax should have —but did not— promptly detect wrongful activity on its computer systems. Hackers "began their attack no later than early March, more than four months before company officials discovered the intrusion."[19] This timeline aligns with the first reports on the Apache application vulnerability, which Equifax officials have said "was the

---

[13] Press Release, *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX (Sep. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628 ("Equifax Press Release 1").

[14] Equifax Press Release 2, *supra* note 11.

[15] Dan Goodin, *Critical Vulnerability Under "Massive" Attack Imperils High-Impact Sites*, ARS TECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/.

[16] Brian Krebs, *Equifax Hackers Stole 200k Credit Card Accounts in One Fell Swoop,* KREBS ON SECURITY (Sep. 14, 2017), https://krebsonsecurity.com/2017/09/equifax-hackers-stole-200k-credit-card-accounts-in-one-fell-swoop/.

[17] Dan Goodin, *Failure to Patch Two-Month-Old Bug Led to Massive Equifax Breach*, ARS TECHNICA (Sep. 13, 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-breach-caused-by-failure-to-patch-two-month-old-bug/.

[18] Equifax Press Release 2, *supra* note 11.

[19] Dan Goodin, *Massive Equifax Hack Reportedly Started 4 Months Before It Was Detected*, ARS TECHNICA (Sep. 20, 2017), https://arstechnica.com/information-technology/2017/09/massive-equifax-hack-reportedly-started-4-months-before-it-was-detected/.

opening that gave attackers an initial hold in the targeted network."[20] Due to Equifax's failure to properly detect the intrusion, the attackers were likely able to perform "months of painstaking hacking as [they] attempted to escalate their privileges and intrude further into the Equifax network," eventually accessing "numerous database tables in several databases."[21]

31. Third, Equifax should have —but did not— timely notify consumers of the data breach and failed to provide adequate measures for consumers to protect themselves from further harm. Under California law, businesses are required to "disclose any breach of the security of the system following discovery" to any California resident "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[22] This disclosure must be made "in the most expedient time possible and without unreasonable delay," the only exception being if law enforcement determines that "the notification will impede a criminal investigation."[23] The reason for the law is simple: immediate notice of a data breach is critical for victims to obtain the best protection afforded by identity-theft protection services.

32. Equifax waited nearly six weeks after it discovered the data breach to publicly disclose the incident. During this time, millions of consumers remained unaware that their PII had been stolen and was vulnerable to misuse by bad actors. Cybersecurity experts have noted that the "data stolen in the Equifax hack is extremely valuable to cyberthieves" and can be used to max out credit cards, order medical prescriptions, or even pin crimes on the victims.[24] Millions of consumers lost valuable time to get ahead of the hackers and take protective measures due to Equifax's delayed notice to the public.

33. When Equifax finally disclosed the data breach on September 7, 2017, the company set up a breach website at www.equifaxsecurity2017.com that consumers could utilize to identify

---

[20] *Id.*

[21] *Id.*

[22] CAL. CIV. CODE § 1798.82(a)

[23] CAL. CIV. CODE § 1798.82(b)-(c)

[24] David Goldman, *Equifax Hack: What's the Worst that Can Happen?*, CNN TECH (Sep. 11, 2017), http://money.cnn.com/2017/09/11/technology/equifax-identity-theft/index.html.

whether they were victims of the data breach.[25] The website requires consumers to enter in their last name and the last six digits of their SSN. Due to the sensitive nature of the information requested, consumers have to trust they are giving their PII to the right party. However, Equifax has quickly breached that trust by tweeting out a similar-sounding, but wrong web address multiple times over the last several weeks, directing consumers to a phishing website instead.[26] While Equifax has since deleted the tweets, and the phishing website operator has been identified as a non-malicious developer (instead, trying to make a point about Equifax's confusing domain name), Equifax's blunder reflects poorly on the company's breach response systems, especially given that it had over a month to prepare, and does little to reassure consumers that it is serious about remedying the situation.

34. Moreover, Equifax initially charged consumers who were seeking to set up freezes on their credit files in response to the data breach.[27] Only after mounting pressure did Equifax agree to waive the fees, albeit only until November 21, and even still, the company's website continued to charge fees days after the waiver was announced.[28] This follows Equifax's removal of an arbitration clause on its data breach website, which consumers heavily denounced as well.[29] In short, Equifax's handling of its unprecedented data breach demonstrates a short-sighted approach that focuses on limiting Equifax's costs and liabilities, instead of investing in robust response systems designed to mitigate the damage for everyone and restore consumer trust in Equifax.

---

[25] Equifax Press Release 1, *supra* note 13.

[26] Dani Deahl, et al., *For Weeks, Equifax Customer Service Has Been Directing Victims to a Fake Phishing Site*, THE VERGE (Sep. 20, 2017), https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishing-identity-monitoring.

[27] Ron Lieber, *Why the Equifax Breach Stings So Bad*, THE NEW YORK TIMES (Sep. 22, 2017), https://www.nytimes.com/2017/09/22/your-money/equifax-breach.html.

[28] *Id.*

[29] David Lazarus, *The Real Outrage Isn't Equifax's Arbitration Clause - It's All the Others*, LOS ANGELES TIMES (Sep. 12, 2017), http://www.latimes.com/business/lazarus/la-fi-lazarus-equifax-arbitration-clauses-20170912-story.html.

Plaintiff and the Class Suffered Actual and Impending Injuries as a Result of the Data Breach

35. The Equifax data breach was extraordinary—both in the number of consumers affected and the sensitivity of the information involved—and will have devastating consequences for its victims. As World Privacy Forum executive director Pamela Dixon responded, "[t]his is about as bad as it gets."[30]

36. The Equifax data breach exposed highly sensitive PII, which are "the keys that unlock consumers' medical histories, bank accounts and employee accounts."[31] Identity thieves can use the stolen SSNs and related information to perpetrate extensive crimes against Plaintiff and the Class. The data breach allows identity thieves to: (a) open new financial accounts and incur charges in the victims' names; (b) take out loans in the victims' names; (c) open utility accounts; (d) obtain medical services using the victims' information; (e) obtain government benefits posing as the victims; (f) file fraudulent tax returns for the victims to obtain fraudulent refunds; (g) obtain drivers' licenses or identification cards in the victims' names with other persons' pictures; and (h) give false information to the police during an arrest.[32]

37. According to a report issued by former President George W. Bush's Identity Theft Task Force:[33]

> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, … individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to

---

[30] Bernard, *supra* note 9.

[31] *Id.*

[32] *See Taking Charge: What to Do if Your Identity Is Stolen*, U.S. Secret Service, U.S. DEPT. OF HOMELAND SECURITY, *available at* http://www.secretservice.gov/press/Take_Charge.pdf.

[33] *Combating Identity Theft: A Strategic Plan* at 11, THE PRESIDENT'S IDENTITY THEFT TASK FORCE (Apr. 23, 2007), *available at* http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf.

> repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.

38. As a result of Equifax's unreasonable security practices, identity thieves now possess the sensitive PII of Plaintiff and the Class. That information is extraordinarily valuable on the black market and incurs direct costs to Plaintiff and the Class. On the darknet—an underground Internet black market—criminals openly buy and sell stolen credit card numbers, SSNs, and other PII. But credit card numbers alone trade for under $10 on the black market, largely because they are of limited value once the fraud is detected and the card is deactivated by the bank.[34] A card with full personal information (e.g., street address, phone number, and email) fetches more—commonly about $30.[35] The Equifax breach involved the above information, plus driver license numbers in some instances, as well as information on trade lines, credit inquiries, and other public record information that is commonly found in credit reports. Thus, the Equifax breach created a far more valuable treasure trove for criminals. These "complete identity records," unlike simple credit cards, fetch as much as $250-$400 on the black market, making the stolen property of Plaintiff and the Class worth over $35 billion to criminals.

39. Unlike the simple credit-card breaches at retail merchants, these damages cannot be avoided by canceling and reissuing plastic cards. Identity theft is far more pernicious than credit-card fraud. Criminals' ability to open entirely new accounts—not simply prey on existing ones—poses far more dangerous problems. SSNs, unlike credit cards, are not reissued by the government. Identity thieves, especially those with millions of SSN records, can retain the stolen information for years until the controversy has receded. Then, at any moment, the thief can take control of a victim's identity, resulting in thousands of dollars in losses and lost productivity.

40. Class Members' credit profiles can be destroyed before they even realize what happened, and they will be unable to legitimately borrow money, obtain credit, or open bank

---

[34] *The Hidden Data Economy*, MCAFEE LABS (2015), https://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf.

[35] *Id.*

accounts. Class Members can be deprived of legitimate tax refunds or, worse yet, may face state or federal tax investigations due to fraud committed by an identity thief. And even the simple preventive step of adding yourself to a credit-fraud watch list to guard against these consequences substantially impairs Class Members' ability to obtain additional credit. In fact, many experts advise victims to place a freeze on all credit accounts, making it impossible to rent a car, get student loans, buy or rent big-ticket items, or complete a major new car or home purchase.

41. Here, Equifax completely failed to (a) implement a readily available software patch for a known application vulnerability; (b) detect the unauthorized intrusion for over a four-month period; (c) notify consumers in a timely manner as to breaches of their data, and (d) provide an adequate response system that protects consumers from further harm. As a result, Plaintiff and Class Members all must operate under the assumption that their PII was stolen and now face years of credit monitoring costs to protect against any combination of risks involving their PII.

Class Action Allegations

42. Plaintiff brings this class action on behalf of herself and all others similarly situated as members of a proposed Class and Subclass, defined as follows:

> **Class: All persons who are residents of the United States and its territories whose personally identifiable information and/or financial information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017.**
>
> **California Subclass: All persons who are residents of California whose personally identifiable information and/or financial information was compromised as a result of the data breach first disclosed by Equifax on September 7, 2017.**

43. Excluded from the Class are governmental entities, Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, affiliates, legal representatives, employees, coconspirators, successors, subsidiaries, and assigns. Also excluded from the Class are any judges, justices, or judicial officers presiding over this matter and the members of their immediate families and judicial staff.

44. This action is brought and may properly be maintained as a class action pursuant to FED. R. CIV. P. 23(b)(2) and 23(b)(3). This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of these rules.

45. ***Numerosity Under Rule 23(a)(1).*** The Class is so numerous that the individual joinder of all members is impracticable. While the Class's exact number is currently unknown and can only be ascertained through appropriate discovery, Equifax has estimated that approximately 143 million of its customers are affected nationwide. The California Attorney General has further reported that over 15 million Californians were affected by this data breach. This is more than sufficient to satisfy the numerosity requirement.

46. ***Commonality Under Rule 23(a)(2).*** Common legal and factual questions exist that predominate over any questions affecting only individual Class Members. These common questions, which do not vary among Class Members and which may be determined without reference to any Class Member's individual circumstances, include, but are not limited to:

a. Whether Equifax owed a duty to Plaintiff and the Class to adequately protect their personal and financial information;

b. Whether Equifax owed a duty to provide timely and accurate notice of the data breach to Plaintiff and the Class;

c. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

d. Whether Equifax's security practices were adequate and reasonable to protect the Class's PII in light of industry-standard procedures;

e. Whether Equifax's conduct, including its failure to take reasonable security precautions, resulted in the loss of millions of consumers' PII;

f. Whether Equifax failed to notify consumers of the breach of their PII in violation of the California Data Breach Act, CAL CIV. CODE §§ 1798.80 *et seq.*;

g. Whether Equifax engaged in unfair, unlawful, or deceptive business practices in violation of the UCL, CAL. BUS. & PROF. CODE §§ 17200 *et seq.*;

h. Whether Plaintiff and the Class have been damaged by the wrongs alleged and are entitled to compensatory or punitive damages;

i. Whether Plaintiff and the Class are entitled to injunctive or other equitable relief, including restitution.

47. Each of these common questions is also susceptible to a common answer that is capable of classwide resolution and will resolve an issue central to the validity of the claims.

48. ***Adequacy of Representation Under Rule 23(a)(4).*** Plaintiff is an adequate Class representative because she is a Class Member, and her interests do not conflict with the Class's interests. Plaintiff retained counsel who are competent and experienced in consumer-protection class actions. Plaintiff and her counsel intend to prosecute this action vigorously for the Class's benefit and will fairly and adequately protect the Class's interests.

49. ***Rule 23(b)(2) Injunctive Class.*** The Class can be properly maintained under Rule 23(b)(2). Defendant has acted or refused to act, with respect to some or all issues presented in this Complaint, on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the Class as a whole.

50. ***Rule 23(b)(3) Predominance and Superiority.*** The Class can be properly maintained under Rule 23(b)(3), because the above common questions of law and fact predominate over any questions affecting individual Class Members. A class action is also superior to other available methods for the fair and efficient adjudication of this litigation because individual litigation of each Class Member's claim is impracticable. Even if each Class Member could afford individual litigation, the court system could not. It would be unduly burdensome if thousands of individual cases proceed. Individual litigation also presents the potential for inconsistent or contradictory judgments, the prospect of a race to the courthouse, and the risk of an inequitable allocation of recovery among those with equally meritorious claims. Individual litigation would increase the expense and delay to all parties and the courts because it requires individual resolution of common legal and factual questions. By contrast, the class-action device

presents far fewer management difficulties and provides the benefit of a single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CLAIM FOR RELIEF

Violation of California Data Breach Act, Cal. Civ. Code §§ 1798.80 *et seq.*

51. Plaintiff, individually and on behalf of the California Subclass, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

52. CAL. CIV. CODE § 1798.82 provides, in pertinent part:

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

53. The Equifax data breach constituted a breach of their security system.

54. Plaintiff's name, address, birthdate, SSN, driver license number, and credit information constitute "personal information."

55. Equifax unreasonably delayed informing Plaintiff and the Class about the breach of security of their PII after Equifax discovered that the breach had occurred.

56. Equifax failed to disclose to Plaintiff and the Class, without unreasonable delay and in the most expedient time possible, the breach of security of their PII when Equifax knew or reasonably believed such information had been compromised.

57. Upon information and belief, no law enforcement agency instructed Equifax that notification to Class Members would impede an investigation.

58. Pursuant to CAL. CIV. CODE § 1798.84, "[a]ny waiver of a provision of this title is contrary to public policy and is void and unenforceable," "[a]ny customer injured by a violation of this title may institute a civil action to recover damages," and "[a]ny business that violates, proposes to violate, or has violated this title may be enjoined."

59. Plaintiff and the Class seek damages, equitable relief, and any applicable statutory damages under CAL. CIV. CODE §§ 1798.80 *et seq.*.

SECOND CLAIM FOR RELIEF

Violation of the California UCL,
Cal. Bus. & Prof. §§ 17200 *et seq.*

60. Plaintiff, individually and on behalf of the California Subclass, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

61. Plaintiff has standing to pursue this claim as she has suffered injury in fact and has lost money or property as a result of Defendant's actions as set forth above. All Class Members have been injured by the significant costs of protecting themselves from identity theft.

62. Defendant's actions as alleged in this Complaint constitute an "unlawful" practice as encompassed by CAL BUS & PROF. CODE §§ 17200 *et seq.*, because Defendants' actions violated the California Data Breach Act, CAL CIV. CODE §§ 1798.80 *et seq.*, because they constituted negligence, and because they violated federal law, including the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

63. Defendant's actions as alleged in this Complaint constitute a "fraudulent" practice, because Equifax's failure to adequately disclose its lax security practices was likely to deceive consumers, including Plaintiff and the Class. A reasonable consumer who provides extraordinarily sensitive PII to a credit monitoring company would expect that company to provide adequate, industry-standard security to protect the information. Equifax's failure to disclose these inadequate security practices, especially in light of its commitments to safeguard user data contained in its privacy policy, constitutes a material omission in violation of the UCL.

64. Defendant's actions as alleged in this Complaint constitute an "unfair" practice, because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers whose PII was in Equifax's custody. The harm caused by Equifax's wrongful conduct outweighs any utility of such conduct and has caused —and will continue to cause—substantial injury to the Class. There were ample reasonably available alternatives that would have furthered Equifax's legitimate business practices, including using industry-standard technologies to protect its consumer data (e.g., implementation of a readily available software patch). Additionally, Defendant's conduct was "unfair," because it violated the legislatively declared policies reflected by California's strong data-breach and online-privacy laws, including the California Data Breach Act, CAL. CIV. CODE §§ 1798 *et seq.*, the California Online Privacy Protection Act, CAL BUS. & PROF. CODE § 22575 *et seq.*, and the California constitutional right to privacy, CAL. CONST. art. 1, § 1.

65. As a result of Defendant's unlawful, unfair, and fraudulent conduct, Plaintiff and the Class were damaged. Class Members overpaid Equifax for the price of their credit monitoring services, have been injured by the significant costs of protecting themselves from identity theft, and face ongoing and impending damages related to theft of their PII.

66. Defendant's wrongful business practices constitute a continuing course of unfair competition because, on information and belief, Equifax has failed to remedy the lax security practices or even fully notify all affected Class Members. Plaintiff and the Class seek equitable relief to end Equifax's wrongful practices and require it to maintain adequate and reasonable security measures to protect the PII of Plaintiffs and the Class.

67. Plaintiff and the Class also seek an order requiring Defendants to make full restitution of all monies they have wrongfully obtained from Class Members, along with all other relief permitted under CAL. BUS. & PROF. CODE §§ 17200 *et seq.*

THIRD CLAIM FOR RELIEF

Negligence

68. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

69. By accepting Plaintiff's and Class members' nonpublic PII, Equifax assumed a duty requiring it to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse. This duty included, *inter alia*, maintaining and testing Equifax's security systems and taking other reasonable security measures to protect and adequately secure the personal data of Plaintiff and the Class from unauthorized access and use.

70. Equifax also assumed a duty to timely disclose to Plaintiff and the Class that their PII had been or was reasonably believed to have been compromised. Timely disclosure is imperative so that Plaintiff and the Class can report the theft of their SSNs to the Internal Revenue Service, monitor their credit reports for identity fraud, undertake appropriate measures to avoid unauthorized charges on their debit and credit cards, and change or cancel their debit and credit card PINs to mitigate the risks of fraud.

71. As a credit reporting agency that routinely collects sensitive PII from businesses and consumers alike, Equifax has a special relationship with Plaintiff and the Class. Consumers are required to share sensitive data with Equifax as a condition of their applications for employment, housing, loans, and other pertinent services that rely on judgments of creditworthiness. Although there are other CRAs, consumers often do not have a choice as to which CRA is used to run the credit report unless they are signing up directly with one for a personal service. Therefore, consumers must assume Equifax has relevant PII and must rely on Equifax to safeguard this data. If companies like Equifax are not held responsible for failing to take reasonable security measures to protect their customers' PII, consumers will not be protected against future data breaches. The policy of preventing future harm thus supports finding a special relationship between Equifax and the Class.

72. Equifax breached its duty to exercise reasonable care in protecting the PII of Plaintiff and the Class by failing to implement and maintain adequate security measures to safeguard its consumers' data and failing to monitor its computer systems to detect suspicious activity.

73. Equifax further breached its duty of care by failing to promptly and completely inform Plaintiff and the Class that their PII had been stolen, even though Equifax was aware of the breach of its network security as early as July 29, 2017.

74. As a direct and proximate result of Equifax's failure to take reasonable care and use, at a minimum, industry-standard measures to protect the PII in its care, Plaintiff and the Class had their PII stolen, causing direct and measurable monetary losses, threat of future losses, identity theft, and the threat of future identity theft. Based on the previous attacks Equifax suffered and the repeated warnings from regulators that companies handling SSNs were at an increased risk of having their data stolen, especially via hacking, it was reasonably foreseeable that attackers would attempt to penetrate Equifax's security again through a known application vulnerability. It was also reasonably foreseeable that, if Equifax failed to implement reasonable security measures to protect against such attacks, the PII of its consumers would be compromised. Equifax knew—or should have known—that it needed to take adequate and reasonable precautions.

75. Plaintiff and the Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a direct result of Equifax's negligence. This includes identity theft, damage to credit scores and reports, time and expenses resolving fraud claims, and the costs of purchasing credit monitoring services not otherwise necessary.

FOURTH CLAIM FOR RELIEF

Negligence *Per Se*

76. Plaintiff, individually and on behalf of the Class, incorporates by reference all of the allegations contained in the preceding paragraphs of this Complaint.

77. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Equifax had a duty to keep and protect the personal information of its customers.

78. Equifax violated the Gramm-Leach-Bliley Act by failing to ensure the security and confidentiality of its consumer records, failing to protect against any anticipated threats or hazards to the security or integrity of such records, and failing to protect against unauthorized access or use of such records, which resulted in substantial harm to the Class.

79. Equifax's failure to comply with the Gramm-Leach-Bliley Act and applicable federal and state standards and regulations constitutes negligence *per se*.

Prayer for Relief

Plaintiff, on behalf of herself and the Class, request that the Court order the following relief and enter judgment against Defendant as follows:

A. An order certifying the proposed Class under FED. R. CIV. P. 23;

B. An order appointing Plaintiff and her counsel to represent the Class;

C. A declaration that Defendant has engaged in the illegal conduct alleged;

D. An order that Defendant be permanently enjoined from its improper conduct;

E. A judgment awarding Plaintiff and the Class restitution and disgorgement of all compensation obtained by Defendant from its wrongful conduct;

F. A judgment awarding Plaintiff and the Class compensatory, statutory, and punitive damages in amounts to be proven at trial;

G. Prejudgment and postjudgment interest at the maximum allowable rate;

H. Attorneys' fees and expenses and the costs of this action; and

I. All other relief that the Court deems necessary, just, and proper.

Demand for Jury Trial

Pursuant to FED. R. CIV. P. 38(b), Plaintiff hereby demands a trial by jury.

DATED: September 26, 2017

SCHUBERT JONCKHEER & KOLBE LLP

BY: /s/ Noah M. Schubert
NOAH M. SCHUBERT (NO. 278696)

Robert C. Schubert (No. 62684)
Willem F. Jonckheer (No. 178748)
Noah M. Schubert (No. 278696)
Cassidy Kim (No. 315236)
Schubert Jonckheer & Kolbe LLP
Three Embarcadero Ctr Ste 1650
San Francisco, CA 94111-4018
Ph: 415-788-4220
Fx: 415-788-0161
rschubert@sjk.law
wjonckheer@sjk.law
nschubert@sjk.law
ckim@sjk.law

Attorneys for Plaintiff Asha Goldweber and the Class